Claims

What is claimed is:

1. A method for generating an authentication code associated with an entity, the method comprising the steps of:

retrieving a stored secret associated with an entity;

determining a dynamic value associated with a time interval;

retrieving a first generation value indicative of a number of previous authentication code generations;

receiving a personal identification number (PIN);

generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN; and

generating a second generation value responsive to receipt of the PIN.

2. The method of claim 1 further comprising the step of receiving verifier information, and wherein the generating step comprises combining the stored secret, the dynamic value, the first generation value, the PIN, and the verifier information.

3. The method of claim 2 wherein the step of generating the authentication code comprises:

combining the stored secret and the dynamic value to form a first result;

combining the verifier information with the first result to form a second result; and

combining the first generation value with the second result.

4. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the PIN to form a first result;

combining the dynamic value with the first result to form a second result; and

combining the first generation value with the second result.

5. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the first generation value to form a first result;

combining the dynamic value with the first result to form a second result; and

combining the PIN with the second result.

6. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the dynamic value to form a first result; and

combining the first generation value with the first result.

7. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the first generation value to form a first result; and

combining the dynamic value with the first result.

8. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the dynamic value and the first generation value to form a first result; and

combining the stored secret with the first result.

9. The method of claim 1 wherein the step of determining the dynamic value comprises determining a dynamic value responsive to a time-based counter.

10. The method of claim 1 wherein the step of determining a generation value comprises incrementing a generation counter for an authentication code generated during the time interval.

11. The method of claim 10, further comprising the step of resetting the generation counter at the start of a second time interval.

12. The method of claim 1 further comprising the step of the displaying the authentication code on a display.

13. The method of claim 1, wherein the PIN is retrieved from a data store.

14. The method of claim 1, further comprising the step of selecting a combination function based on the first generation value.

15. The method of claim 1, wherein step of retrieving a stored secret comprises retrieving one of a plurality of stored secrets based on the first generation value.

16. The method of claim 1, wherein step of retrieving a generation value comprises retrieving a first generation value indicative of a number of previous code generations within the time interval..

17. A system for generating an authentication code associated with an entity, the system comprising:

a memory element storing a secret associated with an entity;

a dynamic value subsystem determining a dynamic value associated with a time interval;

a personal identification number (PIN) subsystem receiving a PIN;

a first generation value subsystem determining a first generation value indicative of a number of previous authentication code generations within the time interval and calculating a second generation value responsive to receipt of the PIN by the PIN subsystem; and

a combination subsystem generating an authentication code by retrieving the secret from the memory element and combining the secret with the dynamic value from the dynamic value subsystem, the PIN received by the PIN subsystem, and the generation value from the generation value subsystem.

18. The system of claim 17 wherein the PIN subsystem further comprises a keypad.

19. The system of claim 17 wherein the combination subsystem combines the stored secret and the dynamic value to form a first result, combines the PIN with the first result to form a second result, and combines the first generation value with the second result.

20. The system of claim 17 wherein the combination subsystem combines the stored secret and the PIN to form a first result, combines the dynamic value with the first result to form a second result, and combines the first generation value with the second result.

21. The system of claim 17 wherein the combination subsystem combines the stored secret and the first generation value to form a first result, combines the dynamic value with the first result to form a second result, and combines the PIN with the second result.

22. The system of claim 17 wherein the combination subsystem combines the stored secret and the dynamic value to form a first result, and combines the first generation value with the first result.

23. The system of claim 17 wherein the combination subsystem combines the stored secret and the first generation value to form a first result, and combines the dynamic value with the first result.

24. The system of claim 17 wherein the combination subsystem combines the dynamic value and the first generation value to form a first result, and combines the stored secret with the first result.

25. The system of claim 17 wherein the dynamic value subsystem comprises a time-based counter, and the dynamic value subsystem determines a dynamic value responsive to the counter.

26. The system of claim 17 wherein the generation value subsystem comprises a generation counter that is incremented for each generation of the authentication code during the time interval.

27. The system of claim 26, wherein the generation value subsystem resets the generation counter at the start of a second time interval.

28. The system of claim 17 further comprising a display for displaying the generated authentication code.

29. The system of claim 17 wherein the generation value subsystem changes the generation value upon activation of a button.

30. The system of claim 17 wherein the PIN subsystem further comprises a data store for storing the PIN associated with a user.

31. The system of claim 17 wherein the first generation value subsystem determines a first generation value indicative of a number of previous authentication code generations within the time interval.